UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/993,163	11/16/2001	Michael M. Oberberger	IGT1P035X1/P-311CIP	8483

22434 7590 01/21/2004

BEYER WEAVER & THOMAS LLP
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER	
ASHBURN, STEVEN L	
ART UNIT	**PAPER NUMBER**
3714	8

DATE MAILED: 01/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/993,163	OBERBERGER ET AL.	
	Examiner	Art Unit	
	Steven Ashburn	3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-65* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2-7*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b). Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1, 12, 13 and 32-34 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,394,907 to Rowe (May 28, 2002).

Although the conflicting claims are not identical, they are not patentably distinct from each other because the '907 patent claims all the features of the present claims except cashless gaming devices and a network. Regardless, it is implicit in the '907 patent, wherein a network interface allows cashless transaction between gaming properties, that the network interfaces gaming devices to a network. Hence, it would have been obvious to an artisan at the time of the invention to modify the system claimed in the '907 patent to add the features of cashless gaming devices and a network and thereby enhance the

cashless transaction system by networking gaming devices located at different properties to provide a central location for storing cashless gaming data.

Claims 2-11, 14-20, 28 and 35-39 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,394,907 to Rowe (May 28, 2002) in view of Schneier B., "Applied Cryptography, Second Ed.", 1996, Applied Cryptography, Protocols, Algorithms and Source Code in C (*"Schneier"*)

The '907 patent claims all the features of the instant claims except the specific steps of a public key encryption process in which the sender is authenticated. Public-key encryption is well know. *Schneier* teaches that public-key encryption methods were invented in 1976. *See p. 31.* In general, a sending-party communicates securely across a network with a receiving-party in the following manner: (i) the receiving-party provides a public or private encryption key to the sending-party; (ii) the sending-party uses the key to encrypt its data and then sends the data to the receiver; (iii) the receiving-party decrypts the data using its corresponding private or public key. Most commonly, public keys are acquired by accessing a database located somewhere in the system. *See p. 32.* In addition, *Schneier* describes authenticating the sender of keys to further enhance the data's security. *See p. 35.* In view of *Schneier*, it would have been an obvious design choice for an artisan at the time of the invention to modify the '907 patent to employ a public key encryption and authenticate the sender. As suggested by *Schneier*, employing a public key encryption system provides an effective means of encrypting information in a manner that only the receiving-party can decode data and also authenticate the sending-party. *See id.* As a result, the transaction system would be enhanced by protecting the transmitted data from third-parties attempting to defraud the system by intercepting transmitted data.

Claims 21-31 and 40 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,394,907 to Rowe (May 28, 2002) in view of *Schneier*, as applied to claims * above, in further view of Fox et al., U.S. Patent 6,560,581 B1 (May 6, 2003).**

The cashless transaction system suggested by the '907 patent in view of *Schneier* describes all the features of the claims except a message including an encrypted symmetric encryption key. *Fox* discloses an analogous system for secure electronic transactions. It describes securing a message using an encrypted symmetric encryption key to ensure only a particular recipient can decrypt the contents of the message. *See fig. 4-8; col. 2:55-3:3:12.* In view of *Fox*, it would obvious to one of ordinary skill in the art at the time of the invention to modify cashless transaction system suggested by the '907 patent in view of *Schneier*, wherein messages are encrypted before transmission across a network, to add the feature of having messages include an encrypted symmetric encryption key to enhance security by ensuring only a particular recipient can decrypt the contents of the message .

Claims 50-54 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,394,907 to Rowe (May 28, 2002) in view of *Schneier*, as applied to claim 15 above, in further view of Gennaro et al., U.S. Patent 5,937,066 (Aug. 10, 1999).

The cashless transaction system suggested by the '907 patent in view of *Schneier* describes all the features of the claim except a seed shared between parties used to generate an encryption key. *Gennaro* discloses an analogous encryption system. It teaches that it is known in the art to generate a seed shared between parties to provide an encryption key which allows the key to be regenerated at a later time to allow authorities to decode encrypted data if necessary. *See col. 1:61-4:18.* In view of *Gennaro* it would

have been obvious to an artisan at the time of the invention to modify cashless transaction system suggested by the '907 patent in view of *Schneier*, wherein authentication information is encoded using symmetric encryption keys, to add the feature of a seed shared between parties used to generate the encryption key in order to allow authorities to recreate keys for decrypting the cashless transaction data and thereby enforce laws and regulations concerning the data.

Claims 55-65 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-45 of U.S. Patent No. 6,394,907 to Rowe (May 28, 2002) in view of *Schneier* and *Fox*, as applied to claim 21 above, in further view of Gennaro et al., U.S. Patent 5,937,066 (Aug. 10, 1999).

The cashless transaction system suggested by the '907 patent in view of *Schneier* and *Fox* describes all the features of the claim except a seed shared between parties used to generate an encryption key. *Gennaro* discloses an analogous encryption system. It teaches that it is known in the art to generate a seed shared between parties to generate an encryption key which allows the key to be regenerated at a later time to allow authorities to decode encrypted data if necessary. *See col. 1:61-4:18.* In view of *Gennaro* it would have been obvious to an artisan at the time of the invention to modify cashless transaction system suggested by the '907 patent in view of *Schneier*, wherein authentication information is encoded using symmetric encryption keys, to add the feature of a seed shared between parties used to generate the encryption key in order to allow authorities to recreate keys for decrypting the cashless transaction data and thereby enforce laws and regulations concerning the data.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 9-13 and 32-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Klayh, U.S. 2003/0050831 A1.

Claim 1: As listed below, *Klayh* teaches each and every feature of the claim:

a. A network interface allowing a cashless instrument transaction clearinghouse to communicate with each of separate properties. *See fig. 1; ¶¶ 22, 37-39, 63.*

b. A processor configured to (i) receive cashless instrument validation requests via a network interface from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and send information via the network to the second property to approve or reject the cashless instrument validation request. *See fig. 1(3); ¶ 63, 64, 71, 72.* It goes without saying that the request will be approved or rejected based on (i) successful validation of a user's identification or (ii) successful decryption of the data transmitted to the clearinghouse.

c. At least on cashless game device located at each or the plurality of separated properties the communicates with a cashless instrument clearinghouse. *See fig. 1; ¶ 64.*

d. A network allowing communication between the cashless instrument clearinghouse and the cashless gaming device.

Notably, the cashless transaction clearinghouse disclosed by *Klayh* is embodied in game arcades not gaming casinos. Regardless, for the purposes of the claimed system, game arcade and gaming casinos are equivalent. Hence, the claimed invention in unpatentable because *Klayh* anticipates every feature of the claim.

Claim 9: A cashless device encrypting and decrypting cashless transaction information. *See ¶¶ 42, 93.*

Claim 10: A processor further configured to encrypt and decrypt cashless transaction information. *See id.*

Claim 11: A network comprising a local area network, wide area network, the internet and combinations thereof. *See fig. 1; ¶ 95.*

Claim 12: A cashless game device selected from the group consisting of a game machine, a hand-held computing device, a clerk validation terminal and a cashless server. *See fig. 1(11,19,27).*

Claim 13: A processor configured to allow promotional credits issued to cashless instruments at a first property to be used for game player at a second gaming property. *See ¶ 13.*

Claim 32: As listed below, *Klayh* teaches each and every feature of the claim:

a. Generating cashless transaction information. *See fig. 1; ¶¶ 22, 37-39, 63.*

b. Encrypting cashless transaction information. *See ¶ 93.*

c. Sending a message addressed to a second game property with al least the cashless transaction information to the cashless transaction clearinghouse. *See fig. 1;* ¶¶ *22, 37-39, 63.*

d. Cashless transaction clearinghouse receives an instrument validation requests via a network interface from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property; and sends information via the network to the second property to approve or reject the cashless instrument validation request. *See fig. 1(3);* ¶ *63, 64, 71, 72.* It goes without saying that the request will be approved or rejected based on successful validation of a user's identification or successful decryption of data. Notably, the cashless transaction clearinghouse disclosed by *Klayh* is embodied in game arcades not gaming casinos. Regardless, for the purposes of the claimed system, game arcade and gaming casinos are equivalent. Hence, the claimed invention in unpatentable because *Klayh* anticipates every feature of the claim.

Claim 33: Generating a first message. *See id.*

Claim 34: A cashless game device selected from the group consisting of a game machine, a hand-held computing device, a clerk validation terminal and a cashless server. *See fig. 1(11,19,27).*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-8, 14-20, 28 and 35-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier B., "Applied Cryptography, Second Ed.", 1996, Applied Cryptography, Protocols, Algorithms and Source Code in C (*"Schneier")*

Schneier discloses methods for encrypting information transmitted over networks from sending-party to a receiving party. In a public-key encryption system, *Schneier* teaches encrypting data using pair of keys comprised of a "public-key" and "private-key". *See pp.31-34.* Typically, a public key is made available for encrypting messages whereas a private-key is held private for decrypting the messages encoded with the public-key; hence the names. *See id.* Because the keys function as a pair, either key may be used for encrypting the information. *See id.* The keys may be stored at either the sending-party and receiving party. *See pp. 31-34.* Most commonly, the public keys are stored in a database accessible by a sending party so that the sender can encrypt data without requesting a key from a receiving party for each encryption. *See pp. 31-32.* This database can be located anywhere in the in the system. *See id.*

Claim 2: *Klayh* discloses all the features of the claim except having the clearinghouse store public encryption keys for each of the gaming devices. In this case, the sending-party is a gaming device and the receiving-party is the clearinghouse. In view of *Schneier*, it would have been an obvious design choice for an artisan at the time of the invention to modify the *Klayh*, in which game data is encrypted before transmission across a network, to add the feature of having the clearinghouse store public encryption keys for each of the devices. As suggested by *Schneier*, employing a public key encryption system provides an effective means of encrypting information because the receiver can decode data transmitted by a sending-party without revealing its private key. *See id.* Moreover, storing public keys in a central location makes the system more convenient because it allows a sending-party to acquire a public key with no prior arrangements. *See id.*

Claim 3: *Schneier* teaches public key encryption that decrypts data encrypted with a private encryption key using a corresponding public encryption key and encrypting data using public encryption keys. *See pp. 31-34.* Encryption or decryption may be performed using either the public or private encryption keys. Whether to use one or the other is a matter of design choice. Hence in the cashless game system described by *Klayh* in view of *Schneier*, wherein public key encryption is used to secure cashless game data, it would be obvious design choice for an artisan at the time of the invention to rearrange the steps of the process to decrypt cashless data encrypted with a private encryption key using a corresponding public encryption key and encrypting data using public encryption keys.

Claim 4: *Schneier* teaches storing a private encryption key. *See id.*

Claim 5: *Schneier* teaches public key encryption that decrypts data encrypted with a public encryption key using a corresponding private encryption key and encrypting data using private encryption keys. *See pp. 31-32.* In fact, encryption or decryption may be performed using either the public or private encryption keys. Whether to use one or the other is a matter of design choice. Hence in the cashless game system described by *Klayh* in view of *Schneier*, wherein public key encryption is used to secure cashless game data, it would be obvious design choice for an artisan at the time of the invention to rearrange the steps of the process to decrypt cashless data encrypted with a public encryption key using a corresponding private encryption key and encrypting data using private encryption keys.

Claim 6: *Schneier* teaches storing a public encryption keys and a private encryption keys at either/or the sending-party and receiving party. *See pp. 31-34.* In addition, *Schneier* teaches storing public encryption keys for a sending-party in a database located somewhere in the system. *See p. 32.*

Hence in the cashless game system described by *Klayh* in view of *Schneier*, wherein public key encryption is used to secure cashless game data, it would be obvious design choice for an artisan at the time of the invention to rearrange the parts to storing a clearinghouse public encryption key and gaming device encryption key at the gaming device.

Claim 7: *Schneier* teaches public key encryption that decrypts data encrypted with a private encryption key using a corresponding public encryption key and encrypting data using public encryption keys. *See pp. 31-32.* In fact, encryption or decryption may be performed using either the public or private encryption keys. Whether to use one or the other is a matter of design choice. Hence in the cashless gaming system described by *Klayh* in view of *Schneier*, wherein public key encryption is used to secure cashless game data, it would be obvious design choice for an artisan at the time of the invention to rearrange the steps of the process to decrypt cashless data encrypted with a private encryption key using a corresponding public encryption key and encrypting data using public encryption keys.

Claim 8: *Schneier* teaches public key encryption that decrypts data encrypted with a public encryption key using a corresponding private encryption key and encrypting data using private encryption keys. *See pp. 31-32.* In fact, encryption or decryption may be performed using either the public or private encryption keys. Whether to use one or the other is a matter of design choice. Hence in the cashless gaming system described by *Klayh* in view of *Schneier*, wherein public key encryption is used to secure cashless game data, it would be obvious design choice for an artisan at the time of the invention to rearrange the steps of the process to decrypt cashless data encrypted with a public encryption key using a corresponding private encryption key and encrypting data using private encryption keys.

Claim 14: *Klayh* teaches encrypted cashless game clearinghouse data with an encryption key from each location. *See ¶¶ 22, 37-39, 63, 71, 93.* The system receives cashless instrument validation requests via a network interface from a first property for a cashless instrument presented at the first property where the cashless instrument was generated at a second property and sends information via the network to the second property to approve or reject the cashless instrument validation request. *See fig. 1(3); ¶ 64, 71.* However, unlike the applicant's claim, *Klayh* does not describe the specific steps of a public key encryption process in which the sender is authenticated.

Public-key encryption is well know. *Schneier* teaches that public-key encryption methods were invented in 1976. *See p. 31.* In general, a sending-party communicates securely across a network with a receiving-party in the following manner: (i) the receiving-party provides a public or private encryption key to the sending-party; (ii) the sending-party uses the key to encrypt its data and then sends the data to the receiver; (iii) the receiving-party decrypts the data using its corresponding private or public key. Most commonly, public keys are acquired by accessing a database located somewhere in the system. *See p. 32.* In addition, *Schneier* describes authenticating the sender of keys to further enhance the data's security. *See p. 35.*

In this claim, the clearinghouse is the receiving-party and the game device is the sending-party. Hence, in view of *Schneier*, it would have been an obvious design choice for an artisan at the time of the invention to modify the *Klayh*, in which game data is encrypted with a key before transmission across a network, employ public key encryption and authenticate the sender. As suggested by *Schneier*, employing a public key encryption system provides an effective means of encrypting information because the receiver can decode data transmitted by a sending-party without revealing its private key. *See id.*

Claim 15: As discussed above, *Klayh* teaches all the features of the claim except authenticating the identity of a sending-party. *Schneier* teaches a public-key encryption system that enhances the

security of a transmission by identifying the sending-party with a digital signature. *See p. 37.* Hence, in view of *Schneier*, it would have been an obvious for an artisan at the time of the invention to modify the *Klayh*, in which game data is encrypted with a key before transmission across a network, to employ public key encryption wherein the identity of the sending-party is authenticated . As suggested by *Schneier*, authenticating the sending-party in a public-key encryption system enhances security by verifying the source of a message and thereby preventing spoofing of the system by a third party.

Claim 16: *Klayh* discloses operating on a cashless transaction information. *See fig. 1; ¶¶ 22, 37-39, 63.* Notably, the type of information is irrelevant because all data is the equivalent. Hence, classifying the data as cashless is meaningless.

Claim 17: *Klayh* discloses storing cashless transaction information. *See fig. 1; ¶¶ 22, 37-39, 63.* Notably, the type of information is irrelevant because all data is the equivalent. Hence, classifying the data as cashless is meaningless. Furthermore, storing data is inherent in a data-processing system because, at a minimum, the data is storied in data registers for processing.

Claim 18: *Klayh* discloses translating information from a first format used by first gaming property to a second format used by a second gaming property by way of a software shell using a particular communication protocol which is located between a property and the clearinghouse. *See* ¶¶ 42, 46. Notably, this feature is implicit in *Klayh's* system. If the system was not required to translate formats between properties, neither *Klayh* nor the claimed invention would be distinguishable from a typical network of cashless devices using debit cards.

Claim 19: *Schneier* discloses that information encryption may be performed using a symmetric encryption key, public-private encryption keys, or a combination thereof. *See pp. 31-38.* In this claim, it would be an obvious design choice to use symmetric encryption keys in the system disclosed by *Klayh*, wherein information is encrypted using a key before transmission, to encrypt a message.

Claim 20: *Schneier* discloses that information encryption may be using a symmetric encryption key, public-private encryption keys, or a combination thereof. *See pp. 31-38.* In this claim, it would be an obvious design choice to use public-private encryption key pairs in the system disclosed by *Klayh*, wherein information is encrypted using a key before transmission, to encrypt a message.

Claim 28: *Schneier* describes signing documents with symmetric encryption keys wherein a first symmetric encryption key is generated; information in encrypted for a second message with the first symmetric encryption key; encrypting the first symmetric encryption key and generating a second message with the encrypted first symmetric encryption key and the encrypted information. *See pp. 35-36.*

Claim 35: *Schneier* describes encrypting information with one or more symmetric keys, public keys from a public/private pair, private key from a public/private pair or combinations thereof. *See pp 31-38.*

Claim 36: *Schneier* describes receiving a message from a sender and authenticating the identity of the message's sender. *See pp. 35-38.*

Claim 37: *Schneier* describes decrypting information included in a message. *See pp. 34-38.*

Claim 38: *Schneier* describes decrypting messages with one or more symmetric keys, public keys from a public/private pair, private key from a public/private pair or combinations thereof. *See pp 31-38.*

Claim 39: *Schneier* describes generating a symmetric encryption key and encrypting information with the key. *See pp. 31-37.* Although not stated, it is implicit that a symmetric key must be generated at some point in the encryption process.

Claims 21-27, 29-31 and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Klayh* in view of *Schneier*, as applied to claim 15 above, in further view of Fox et al., U.S. Patent 6,560,581 B1 (May 6, 2003).

Claims 21: The cashless transaction system suggested by *Klayh* in view of *Schneier* describes all the features of the claim except a message including an encrypted symmetric encryption key. *Fox* discloses an analogous system for secure electronic transactions. It describes securing a message using an encrypted symmetric encryption key to ensure only a particular recipient can decrypt the contents of the message. *See fig. 4-8; col. 2:55-3:3:12.* In view of *Fox*, it would obvious to one of ordinary skill in the art at the time of the invention to modify cashless transaction system suggested by *Klayh* in view of *Schneier*, wherein messages are encrypted before transmission across a network, to add the feature of having messages include an encrypted symmetric encryption key to enhance security by o ensuring only a particular recipient can decrypt the contents of the message .

Claim 22: *Fox* describes decrypting the symmetric encryption key. *See id.*

Claim 23: *Fox* describes encrypting a symmetric key at a first location using a public-private encryption key pair. *See id.*

Claim 24: *Fox* describes encrypting a symmetric encryption key twice at a first location using a first location public encryption key and decrypting using a private encryption key from a second location. *See id.*

Claim 25: *Fox* describes decrypting a symmetric encryption key at a second location using first location public encryption key and decrypting using a second location private encryption key. *See id.*

Claim 26: *Fox* describes a message encrypted with a symmetric encryption key. *See id.*. Notably, the type of information is irrelevant because all data is the equivalent. Hence, classifying the data as cashless is meaningless.

Claim 27: *Schneier* discloses that information encryption may be using a symmetric encryption key, public-private encryption keys, or a combination thereof. *See pp. 31-38.* In this claim, it would be an obvious design choice to use public-private encryption key pairs in the system disclosed by *Klayh*, wherein information is encrypted using a key before transmission, to encrypt a message.

Claim 29: *Fox* describes a first symmetric encryption key being encrypted at a first location using the first locations private encryption key from a pair and using a public encryption key from a second encryption key pair. *See id.* Either a public or private key from the pair may be used to perform the encryption. The selection is a matter of design choice.

Claim 30: *Fox* describes verifying the authenticity of an originator using by receiving an additionally message from a party comprising encrypted information and encrypted symmetric encryption keys; decrypting the symmetric encryption key and comparing the symmetric keys. *See id.*

Claim 31: *Fox* describes authenticating a party by receiving a message from the party containing a key associated with the party. *See id.*

Claims 40: *Fox* describes encrypted a symmetric encryption key; generating a message with the encrypted key and other data, then ending a message to another party. *See fig. 4-8; col. 2:55-3:3:12.*

Claims 50-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Klayh* in view of *Schneier*, as applied to claim 15 above, in further view of Gennaro et al., U.S. Patent 5,937,066 (Aug. 10, 1999).

Claim 50: The cashless transaction system suggested by *Klayh* in view of *Schneier* describes all the features of the claim except a seed shared between parties used to generate an encryption key. *Gennaro* discloses an analogous encryption system. It teaches that it is known in the art to generate a seed shared between parties to provide an encryption key which allows the key to be regenerated at a later time to allow authorities to decode encrypted data if necessary. *See col. 1:61-4:18.* In view of *Gennaro* it would have been obvious to an artisan at the time of the invention to modify cashless transaction system suggested by *Klayh* in view of *Schneier*, wherein authentication information is encoded using symmetric encryption keys, to add the feature of a seed shared between parties used to generate the encryption key in order to allow authorities to recreate keys for decrypting the cashless transaction data and thereby enforce laws and regulations concerning the data.

Claim 51: The cashless transaction system suggested by *Klayh* in view of *Schneier* and *Gennaro* describes all the features of the claim except a random noise sequence. Regardless, it is notoriously well known to generate numbers using a noise sequence in order to produce a unpredictable, random numbers. Hence, in the cashless transaction system suggested by *Klayh* in view of *Schneier* and *Gennaro*, wherein data message or encryption key includes a random number, it would have been obvious to an artisan at the time of the invention to encrypt random noise sequence to produce a random numbers which cannot be predicted by an eavesdropper and thereby enhance the security of the system by preventing the eavesdropper obtaining the number and defrauding the system.

Claim 52: *Klayh* describes a cashless instrument selected from the group of a smart card, debit card, bar-coded ticket and a ticket voucher. *See ¶¶ 16, 21.*

Claim 53: *Schneier* describes generating an encryption key pair including a public key and private key. *See pp. 31-34.*

Claim 54: *Klayh* describes generating a plurality of messages. *See fig. 1; ¶¶ 22, 37-39, 63.*

Claims 55-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Klayh* in view of *Schneier* and *Fox*, as applied to claim 21 above, in further view of Gennaro et al., U.S. Patent 5,937,066 (Aug. 10, 1999).

Claims 55 and 63: The cashless transaction system suggested by *Klayh* in view of *Schneier* and *Fox* describes all the features of the claim except a seed shared between parties used to generate an encryption key. *Gennaro* discloses an analogous encryption system. It teaches that it is known in the art to generate a seed shared between parties to generate an encryption key which allows the key to be

regenerated at a later time to allow authorities to decode encrypted data if necessary. *See col. 1:61-4:18.* In view of *Gennaro* it would have been obvious to an artisan at the time of the invention to modify cashless transaction system suggested by *Klayh* in view of *Schneier*, wherein authentication information is encoded using symmetric encryption keys, to add the feature of a seed shared between parties used to generate the encryption key in order to allow authorities to recreate keys for decrypting the cashless transaction data and thereby enforce laws and regulations concerning the data.

Claim 56 and 57: *Fox* describes authenticating a party's identity by comparing an information sequence to a public encryption key to determine if the values are identical. *See fig. 8.*

Claim 58: *Schneier* describes generating an encryption key pair including a public key and private key. *See pp. 31-34.*

Claim 59: *Klayh* describes generating a plurality of messages transmitted between a plurality of locations. *See fig. 1; ¶¶ 22, 37-39, 63.*

Claim 60: *Gennaro* discloses receiving a seed. The source of the seed is a matter of design choice.

Claim 61: *Schneier* describes receiving a public encryption key from a receiving-party. In this case, the receiving party would be the clearinghouse.

Claim 62: *Schneier* describes authenticating the identity of the sender of a encryption key. *See pp. 37-38.* In this case, the clearing house would be the sender.

Claim 64: *Schneier* describes storing public encryption keys. *See pp. 31-21.*

Claim 65: *Schneier* describes sending information encrypted with a public key to a receiving party. In this case, the receiving-party is the clearinghouse.

Prior Art, Not Relied On

The following prior art of record is not relied upon but is considered pertinent to applicant's disclosure:

- Thacher et al., U.S. Patent 5,083,271 (Jan, 21, 1992) describes a cashless game system. The patent is incorporated by reference into *Klayh*
- Fertitta, III et al., U.S. Patent 6,302,793 (Oct. 16, 2001) discloses a multi-property player tracking system.
- Davis et al., U.S. Patent 5,544,086 (Aug. 6, 1996) discloses financial transaction systems in which data is stored in central location and transmitted data in encrypted. The discloses system is analogous to the claimed "cashless transaction clearinghouse".
- Akel et al., U.S. Patent 5,457,305 (Oct. 10, 1995) discloses financial transaction systems in which gaming data is stored in central location. The discloses system is analogous to the claimed "cashless transaction clearinghouse".
- Chen, U.S. Patent App. Pub. 2002/0032656 A1 (Mar. 14, 2002) teaches that it was known in the art at the time of the invention to employ networked financial transaction systems in which data is stored in central location. The discloses system is analogous to the claimed "cashless transaction clearinghouse".

- Williams, U.S. Patent App. Pub. 2003/0216967 A1 (Nov. 20, 2003) discloses an customer tracking system in which data is stored in central clearinghouse.
- Baltzley, U.S. Patent 6,154,543 (Nov. 28, 2000) discloses methods for securing and authenticating data transmitted over networks using public-key encryption wherein encrypted keys are encrypted.
- *Introduction to Public-Key Cryptography*, http://developer.netscape.com/docs/manuals/security/-pkin/contents.htm, Oct. 09, 1998, downloaded from the Internet on January 8, 2004 teaches methods for securing and authenticating data transmitted over networks using public-key encryption.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Steven Ashburn whose telephone number is 703 305 3543. The examiner can normally be reached on Monday thru Friday, 8:00 AM to 4:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tom Hughes can be reached on 703-308-1806. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703 308 1148.

s.a.

S. THOMAS HUGHES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3700